Journal scientific and applied research, vol. 6, 2014
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

PERFORMANCE AND CONNECTION ANALYSIS OF THE COMPUTER SYSTEMS AND NETWORKS

Petar Boyanov

DEPARTMENT OF COMMUNICATION AND COMPUTER TECHNOLOGY, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR,
E-mail: peshoaikido@abv.bg

ABSTRACT: *In this paper a performance and connection analysis of determined computer systems and networks is made. Each communication process and state must be daily scanned and analyzed by system administrators, security-professionals and IT specialists. Ensuring a secure flow of computer and network processes and performance is very important priority for many large and small companies and for normal users. Most of the malicious user and programmers use vulnerability in the selected network via determined computer and network processes.*

KEY WORDS: *Computer and network security, Connection analysis, cyber-attacks, Monitoring, Performance, Scanning, Vulnerabilities, Windows 7.*

1. Introduction

Analyzing and monitoring the communication processes and services is the most important task for each system administrator and IT specialist. With a special software environment many computer specialists are able to observe and analyze all of the running communication http requests and to monitor the LAN (Local Area Network), MAN (Metropolitan Area Network) and VPN (Virtual Private Network) connections. This paper is structured as follows. First, in section 2, different network protocol analyzers are compared. After that, in section 3, the wireless network interface of determined host is scanned and monitored. The achieved results are presented in section 4. The final conclusions and recommendations are made in section 5.

2. Related work

In [1] the software product WireShark as a tool for intrusion detection by Usha Banerjee, Ashutosh Vashishtha and Mukul Saxena is presented. In [12]

performance analysis of WireShark in TCP/IP protocol by Shaoqiang Wang, Xu, Yan DongSheng and ShiLiang is explained. In [8] security analysis with Wireshark by Russ Mcree is made. In [11] different ways to secure a determined network by Eric Seagren are presented and compared. In [4] a bottleneck analysis of traffic monitoring using wireshark by A. Dabir and Matrawy is performed and made. In [2] the Wireshark network analysis tool by L. Chapell is presented.

3. Experiment

The experiment in specialized university computer lab is made. The network ID of this LAN is 10.10.0.0/24. The used software is WireShark Protocol Analyzer version 1.6.8 (SVN Rev 42761 from /trunk-1.6) [10],[11],[12],[13]. Initially was necessary to configure the software product. After the successfully installed software product there has occurred an error with the capturing or listening interfaces of the host. One of the way be fixed this problem is to open a command shell with the "Run as administrator" selection in order to start the NPF driver. As is well known Wireshark uses the Windows Packet capture (WinPcap) driver which is called NPF. On fig. 1 the fixed problem with NPF driver is shown.

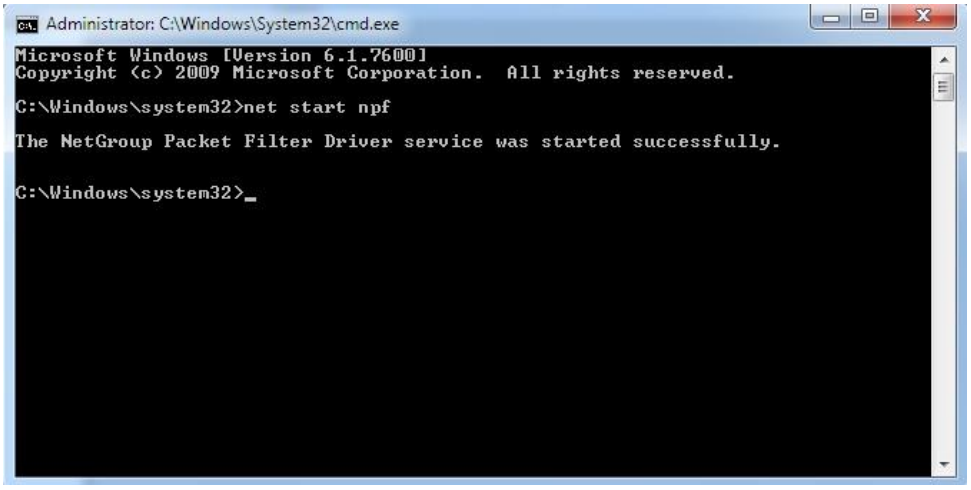

Fig. 1. The successfully started NPF driver

The following experiments only with education intend and purposes are made. The Microsoft Windows 7 Enterprise SP1 operating system in the scanning host has been used. On fig. 2 the interface overview of WireShark is shown.

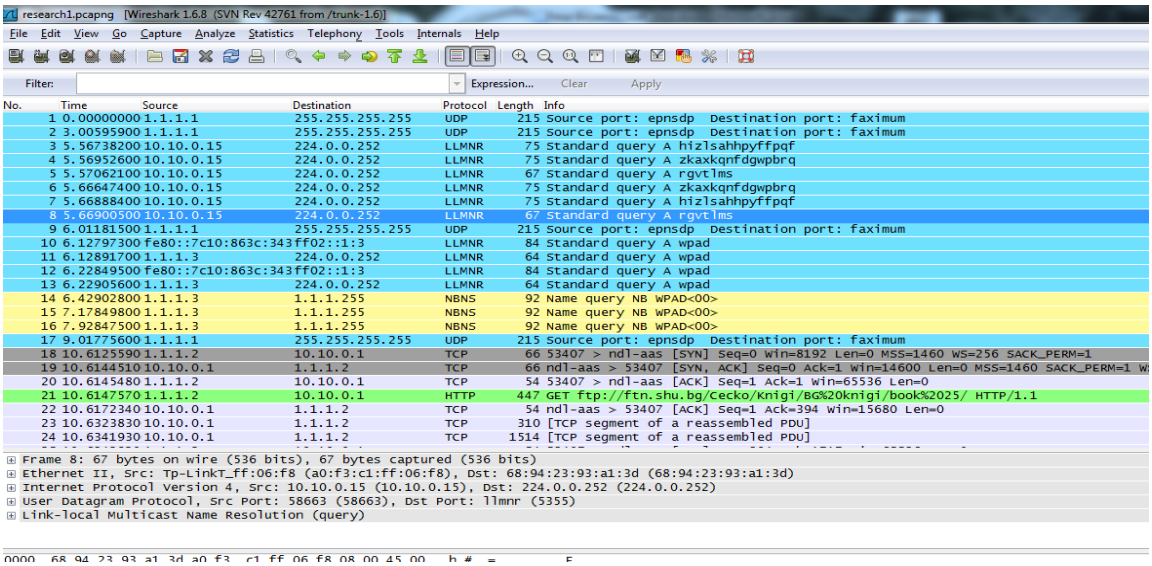

Fig. 2.The interface overview of WireShark

The software product WireShark consists of the following statistics options:

- Summary [8];
- Protocol Hierarchy [2],[3];
- Conversations;
- Endpoints;
- Packet Lengths [4],[5];
- IO (Input Output) graphs [1],[6];
- Conversation lists with Ethernet, IPX, IPv4, IPv6, RSVP, TCP and UDP;
- Service Response Time;
- Compare options;
- Flow graphs [7],[9];
- UDP Multicast Streams;
- WLAN traffic and etc.

On fig. 3 the summary report after the completed scan is shown.

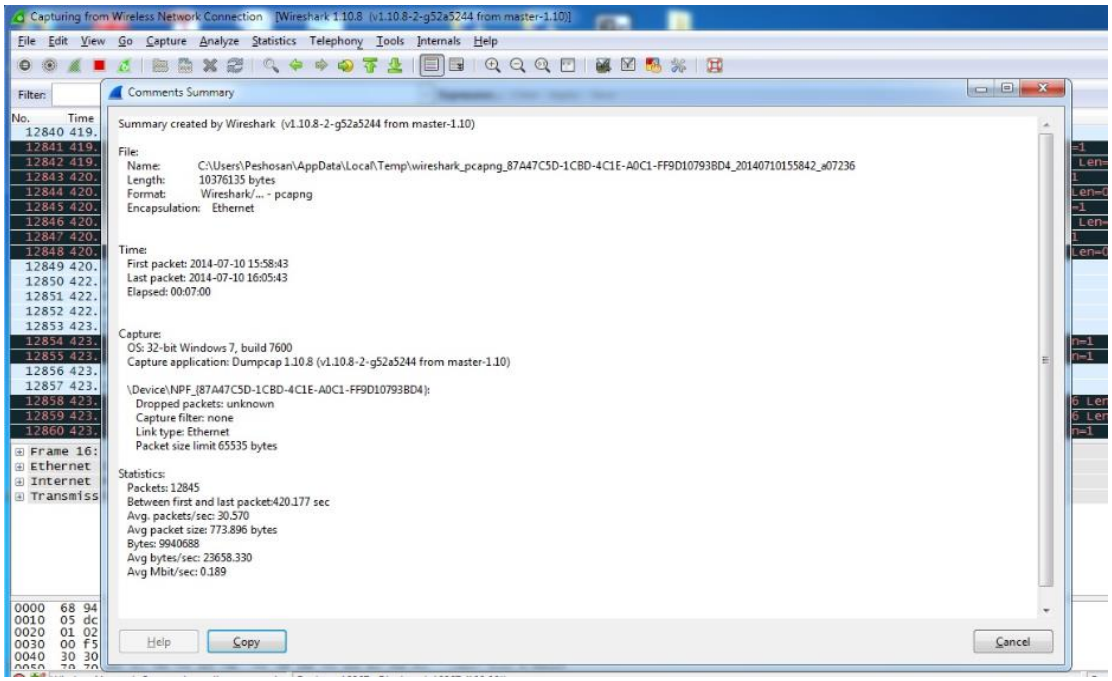

Fig. 3. The summary report after the completed scan

This figure has given information for:

- The name, length, format and encapsulation of the file;
- The time of first and last received packet;
- The Capture operating system - 32-bit Windows 7, build 7600;
- The Capture application - Dumpcap 1.10.8(v1.10.8-2-g52a5244 from master-1.10) and additional statistics parameters.

Other important statistics option is conversation connections (shown on fig. 4).

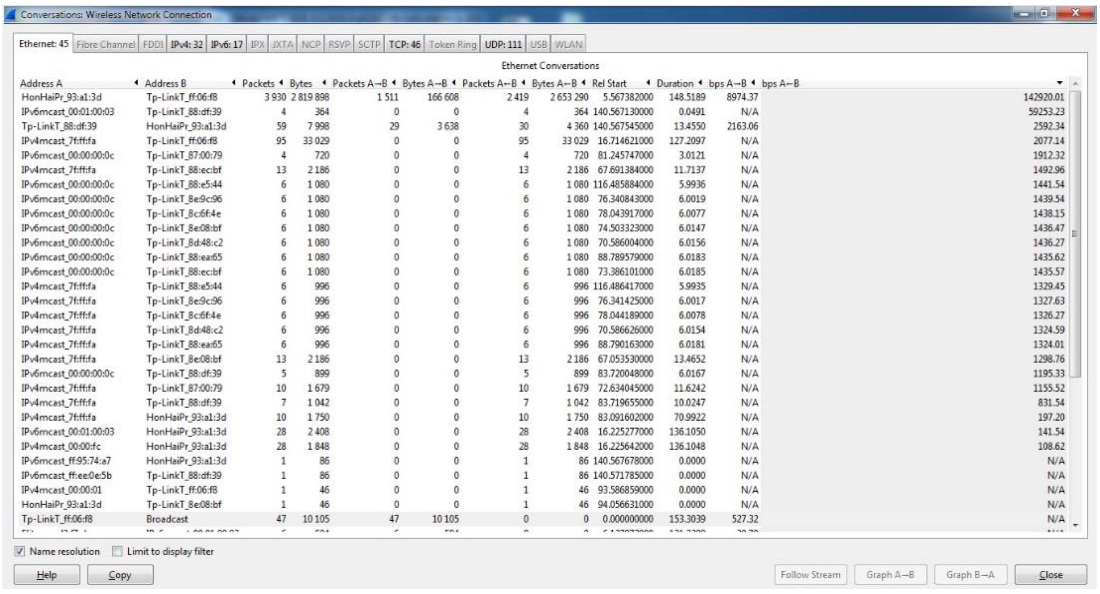

Fig. 4. Conversation for Wireless network connection

This statistics has showed information for IPv4 and IPv6 connections.

On fig. 5 the http request connection by count, rate (ms) and percent are summarized.

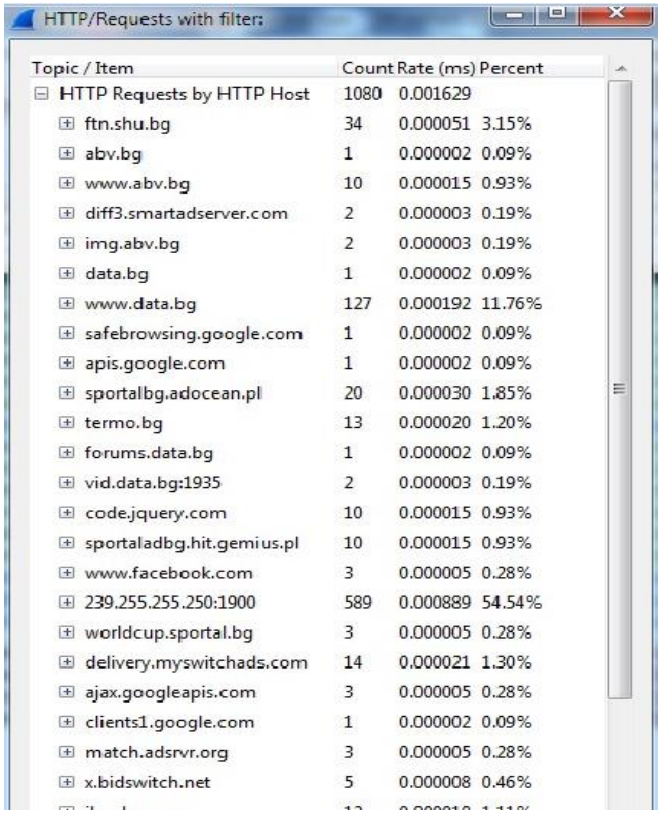

Fig. 5. The http request connection by count, rate (ms) and percent

On fig. 6 the protocol hierarchy statistics is shown.

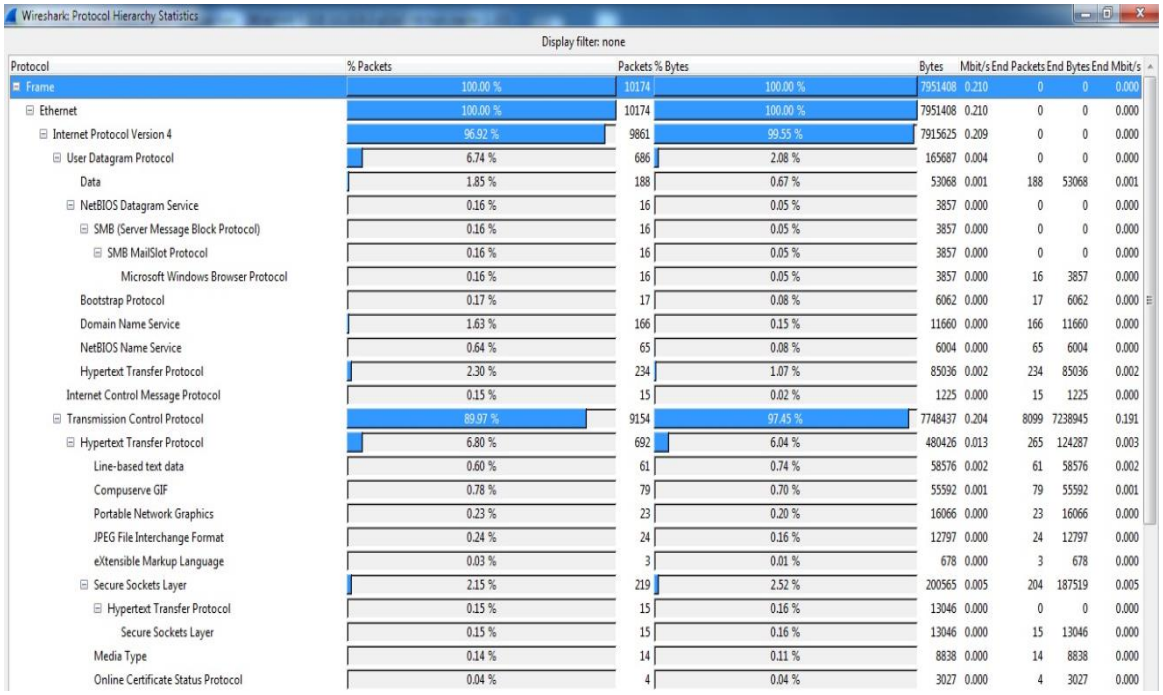

Fig. 6. The protocol hierarchy statistics

This statistics has given detailed information for each network protocol and specifically the all media files and application within.

On fig.7 the IO (Input Output) graph is shown.

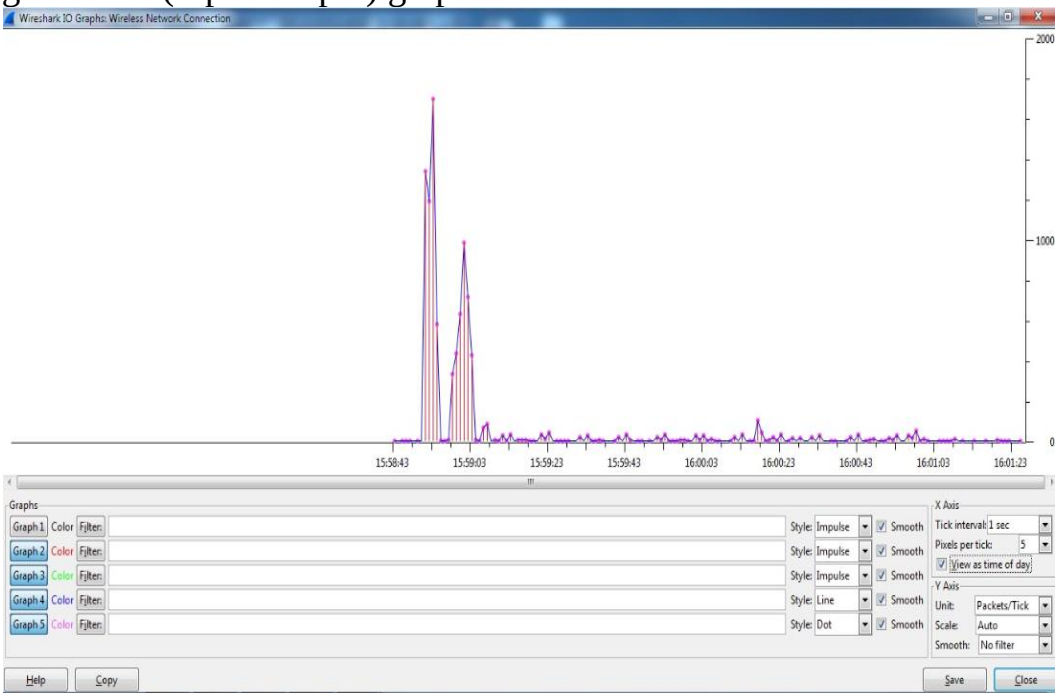

Fig. 7. The IO (Input Output) graph for wireless network connection

4. Results.

Thanks to the achieved scan and observe of the selected wireless network interface each system administrators and IT specialists are able to analyze and summarize all of the active and inactive network connections. Therefore it is recommended and important to be made a baseline network statistics for all connections.

5. Conclusion

In this paper a performance and connection analysis of determined computer systems and networks is made. Thanks to the achieved results for the selected wireless network interface most of the system administrator, IT specialists and cyber professionals have to perform a daily scan all of incoming and outgoing network connection and then to analyze which of them show suspicious, idle or timeout state. The implementation of these mechanisms can provide better protection computer network systems from any malicious cyber-attacks.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young

scientists in the areas of the natural, technical and mathematical sciences". The Project is realized by the financial support of the Operative Program "Development of the human resources" of the European social found of the European Union.

References:

[1] Banerjee, Usha; Vashishtha, Ashutosh; Saxena, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. International Journal of Computer Applications, 2010, 6.7.

[2] Chapell, L. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, Protocol Analysis Institute. EE. UU. Editorial Chapell University, 2010.

[3] Combs, Gerald, et al. Wireshark: Go deep. ArGo Software Design Homepage, 2008, 31.

[4] Dabir, A.; Matrawy, A. Bottleneck analysis of traffic monitoring using wireshark. In: Innovations in Information Technology, 2007. IIT'07. 4th International Conference on. IEEE, 2007. p. 158-162.

[5] Hnatyshin, Vasil Y.; LOBO, Andrea F. Undergraduate data communications and networking projects using opnet and wireshark software. ACM SIGCSE Bulletin, 2008, 40.1: 241-245.

[6] Liu, Lei, et al. Experimental demonstration and comparison of distributed and centralized multi-domain resilient translucent WSON. In: Proceedings of 36th European Conference and Exhibition on Optical Communication (ECOC 2010), paper We. 2010. p. 1-3.

[7] Luo, Qing-Lin, et al. Network protocol parser and verification method based on Wireshark. Computer Engineering and Design, 2011, 32.3: 770-773.

[8] Mcree, Russ. Security Analysis with Wireshark. ISSA Journal, 2006, 39-45.

[9] Munz, Gerhard; CARLE, Georg. Distributed network analysis using TOPAS and Wireshark. In: Network Operations and Management Symposium Workshops, 2008. NOMS Workshops 2008. IEEE. IEEE, 2008. p. 161-164.

[10] Orebaugh, A.; Ramirez, Gilbert; Burke, J. Wireshark. Ethereal network protocol analyzer toolkit. 2006.

[11] Seagren, Eric. Secure your network for free: using NMAP, Wireshark, Snort, Nessus, and MRTG. Syngress, 2007.

[12] Wang, Shaoqiang; Xu, DongSheng; Yan, ShiLiang. Analysis and application of wireshark in TCP/IP protocol teaching. In: E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on. IEEE, 2010. p. 269-272.

[13] WIKI, Wireshark. Ethernet capture setup.[Online] Available at: http://wiki. Wireshark. org. FrontPage [Accessed: 10.09. 2012.].